GRIF 2014

Module SIL

User manual

Version 31 March 2014

Copyright © 2014 Total

Table of Contents

1. Prerequisites and Installation 4
1.1. Prerequisites 4
1.2. Installation of TOTAL version without 4
1.3. Installation of retail version with installer and demonstration version 4
1.4. Saving 4
1.5. Launching 4

2. Presentation 5
2.1. Introduction 5
2.2. Presentation of the graphical user interface 5
2.2.1. Main window of the SIL module 5
2.2.2. Description of the Menus 5
2.2.3. Vertical toolbar 7

3. Configuration of architecture 8
3.1. Architecture definition 8
3.2. Voting for components of a chanel 9
3.2.1. 1oo2S and 1oo2A 9
3.2.2. 2oo3S 10
3.2.3. 2oo3A 11
3.3. Configuration of channels of a part 11
3.4. Take Common Cause Failures into account 11

4. Configuration of components 12
4.1. Configuring the sensors 12
4.2. Configuring the solver 15
4.3. Configuring the actuators 17
4.4. Editing the parameters 20

5. Computes 22
5.1. Launch PFD/PFH computation 22

6. Multi-loop systems 24
6.1. Presentation 24
6.2. Input 24
6.3. Computations 25
6.4. Reports and results 26
6.5. PDF report and MS Excel report 26

7. Charts 27
7.1. Charts Edit window 27
7.2. Editing the curves 28

8. Generating reports 30
8.1. Description 30
8.2. Result SIL 31
8.3. Spurious-trip 32
8.4. PDF reports 32
8.5. Mirosoft Excel XLSX file format export 33

9. Glossary 34
9.1. Format 34
9.2. Definition and explanation of the acronyms and parameters 34

10. Appendix 36
10.1. Configuration of Lambda computation method for CCF 36
10.2. Data Editing Tables 36
10.2.1. Description of the Tables 36
10.2.2. Table accessibility 38
10.3. Options of GRIF - SIL 38

10.3.1. Executables 39
10.3.2. Database 39
10.3.3. Language 39
10.3.4. Options 39
10.3.5. Graphics 40
10.3.6. Digital format 40
10.3.7. Curves 40

1. Prerequisites and Installation

This chapter describes the procedure to follow before the software can be used. Because an external computation engine is used, certain prerequisites are necessary.

1.1. Prerequisites

The minimum hardware requirement is a Pentium IV (or more) with 512 MB memory. Works under Window XP, Vista and 7

1.2. Installation of TOTAL version without

TOTAL's version of the GRIF software does not require an installation procedure. You must unzip the GRIF 201X-Module SIL.zip in the directory of your choice. The path of directory must not contain any special characters such as: {,},[,],(,),$,%, etc.

In the following chapters, we will assume you have unzipped the file in C:\Programmes\Total\GRIF 201X-Module SIL\

1.3. Installation of retail version with installer and demonstration version

The retail version of software is provided with a file whose name is GRIF 201X.zip . Unzip the file (on your desktop for exemple), ans launch GRIF-Install-Win32.exe. A window will guide you through installation step. If you haven't purchase GRIF, please select demo at the end of inttallation.

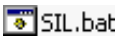
In the following chapters, we will assume you have install GRIF in C:\Programmes\Total\GRIF 201X\

1.4. Saving

Data generated by GRIF are saved in "USER" directory. With Windows XP it is **C:\Documents And Setting \USER**, with Windows Vista and Windows 7 it is **C:\Users\USER**. The name USER is usually your name or your identification number with which you have openned your session on computer.

GRIF Module SIL saves its files in USER/GRIF/SIL/Application

1.5. Launching

The software is now ready for use. To launch the SIL module, double-click on 

qui is in directory where GRIF bas been installed. In retail version, you can also use the Start menu (Sofwares/GRIF 201X).

2. Presentation

2.1. Introduction

This module of GRIF is used for PFD computations. We will focus on the processing of Safety Instrumented Functions (SIF) on continuous process installations (safeties functioning in "on demand mode"). The computations carried out are safety computations; the top event is a non-detected dangerous failure of the SIS safety function.

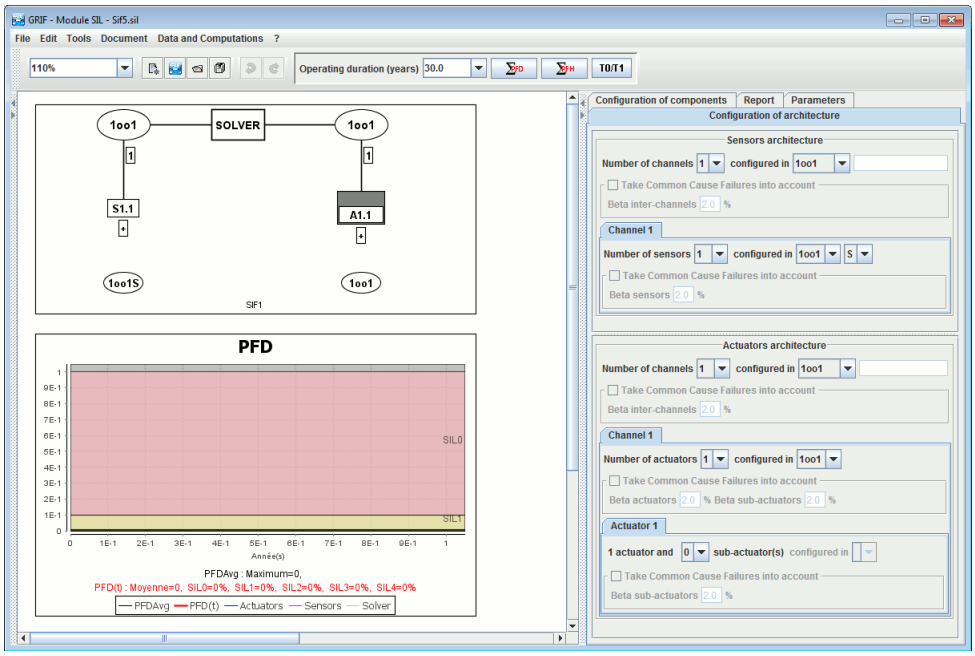
The definitions and parameters used in this document are explained in the glossary (cf Section 9, “Glossary”)

2.2. Presentation of the graphical user interface

2.2.1. Main window of the SIL module

The main window is divided into several parts:

- **Title bar**: The title bar shows the names of the module and file being edited.
- **Menu bar**: The menu bar gives access to all the application's functions.
- **Icon bar (shortcuts)**: The shortcut bar is an icon bar (horizontal) which gives faster access to the most common functions. The **Operating duration** area lets you specify the operating duration in years, and launch computation.
- **Tool bar**: The tool bar (vertical) allows you to select the elements for modeling. By default, this tool bar is not displayed. In order to make it visible, check the box **Display graphical tools bar** in **Tools**.
- **Input zone**: A maximum amount of space has been left for the graphical input zone for creating the model. When module is launched, this zone contains a picture representing the architecture as well as an empty chart as no computations have yet been carried out.
- **Tree**: Graphical tree is between input zone and tool bar. It enables to walk through pages and groups of the document. It is not displayed bt default.
- **Configuration window**: On the right of input zone, a window that contains **Configuration of architecture**, **Configuration of components**, **Report** and **Parameters** enables you to configure the system.

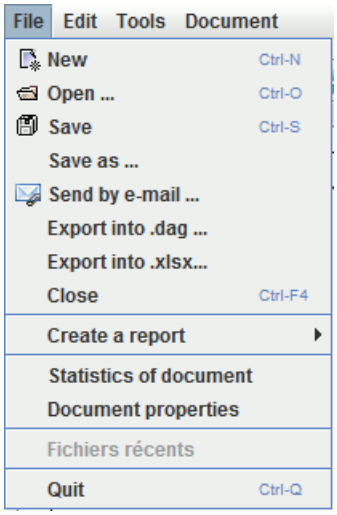


2.2.2. Description of the Menus

1. The **File** menu contains the standard commands used in this type of menu (open, close, save, print, etc.). The properties (name, creation date, created by, description, version) can be accessed and modified by selecting

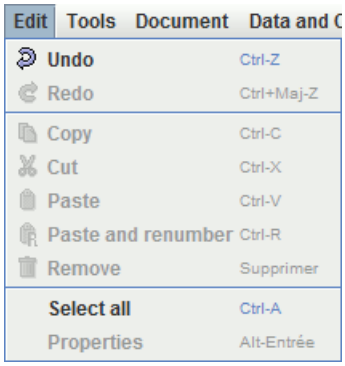
Document properties. The **Document statistics** provide information on the model's complexity. It is also possible to access a certain number (configurable) of recently modified files.

The icon bar just under the menus proposes shortcuts for most of the **File** commands:



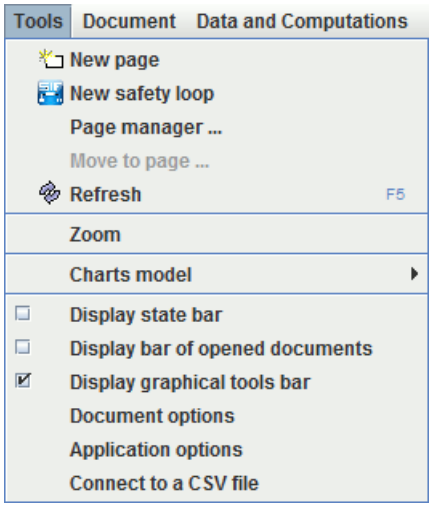
2. The **Edit** menu contains all the commands needed to edit the model being input graphically.

   The icon bar just under the menus proposes shortcuts for most of the **Edit** commands:



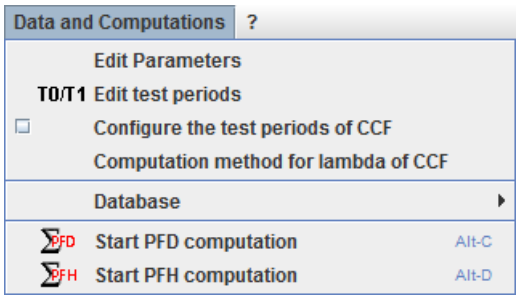
3. The **Tools** menu contains all the commands needed to manage the current model (page management, alignments, options, etc.).

   The icon bar just under the menus proposes shortcuts for most of the **Tools** commands:



4. The **Document** menu gives access to all the documents being created or modified.

5. The **Data and Computations** menu is divided into two parts: data management (creation and management of the different parameters) and configuration/computation launch (computation time, desired computation, etc.)..



The action **Edit of test periods** also available in the toolbar, allows to globally modify the components tests periods.

The action **Configure the test periods of CCF** allows you to manually configure the test periods of CCF. New fields are available on the **Configuration of architecture** panel.

The **Computation method for lambda of CCF** is explained in the chapter Section 10.1, “Configuration of Lambda computation method for CCF”.

6. Finally, the **Help** menu accesses the on-line Help, the Help topics and to "About".

2.2.3. Vertical toolbar

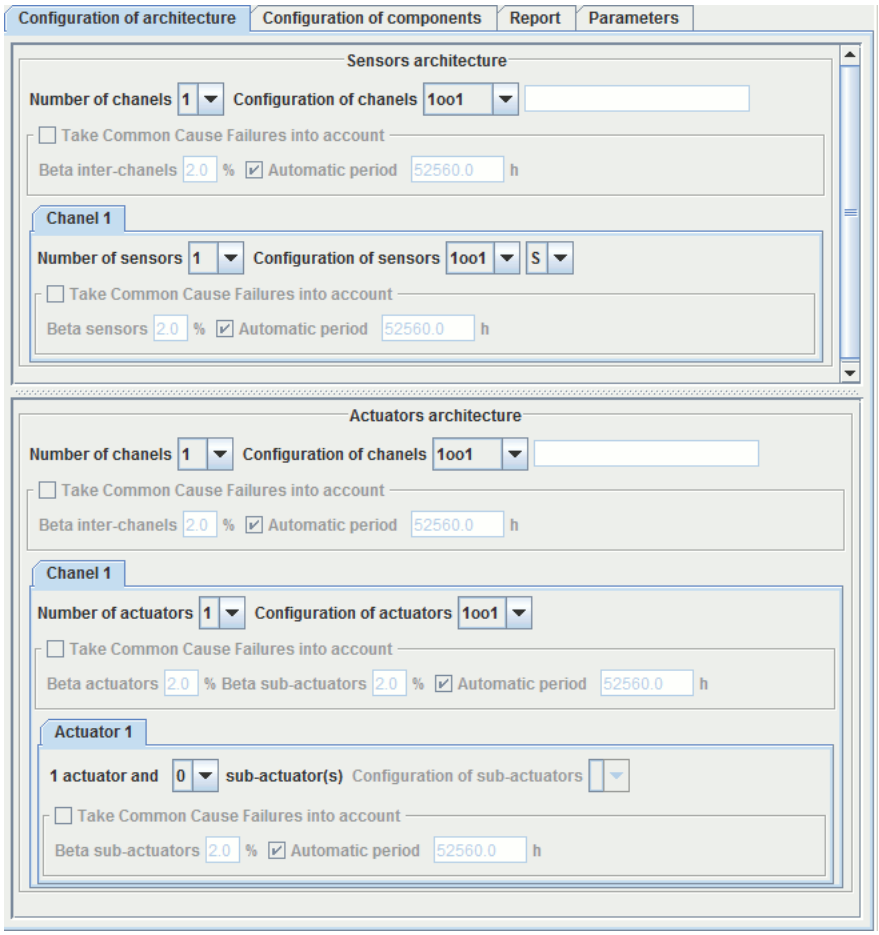
Each operating safety model has its own icons. All the graphical symbols for the event trees are shown on the vertical icon bar on the left of the data input screen. This toolbar is not visible by default, it can be displayed with the **Outils** menu.

The vertical toolbar contains the following items:

- **Select** selects the desired elements.
- **Group** to create a new group. A group is a sub-page which can contains graphics elements.
- **Comment** to add text directly to the graphic.
- **Charts** to draw charts representing computations on the model.
- **Line** to draw lines or arrows.

3. Configuration of architecture

The **Configuration of architecture** tab enables to define architecture. Each modification made on the tab is visible on picture of architecture.


Configuration of architecture
Configuration of components
Report
Parameters
Sensors architecture
Number of chanels 1
Configuration of chanels 1oo1
Take Common Cause Failures into account
Beta inter-chanels 2.0 % Automatic period 52560.0 h
Chanel 1
Number of sensors 1
Configuration of sensors 1oo1 S
Take Common Cause Failures into account
Beta sensors 2.0 % Automatic period 52560.0 h
Actuators architecture
Number of chanels 1
Configuration of chanels 1oo1
Take Common Cause Failures into account
Beta inter-chanels 2.0 % Automatic period 52560.0 h
Chanel 1
Number of actuators 1
Configuration of actuators 1oo1
Take Common Cause Failures into account
Beta actuators 2.0 % Beta sub-actuators 2.0 % Automatic period 52560.0 h
Actuator 1
1 actuator and 0 sub-actuator(s) Configuration of sub-actuators
Take Common Cause Failures into account
Beta sub-actuators 2.0 % Automatic period 52560.0 h

3.1. Architecture definition

The top part of the tab : **Configuration of architecture** enables to define the configuration of sensor part. Possible choices are:

- The number of channels and the (logical) configuration between channels. (cf. **Configuration des canaux**)
- Number of components in each channel and the configuration of these components in the channel.
- Taking Common Cause failure into account for all sensors. (cf. **Configuration des DCC**)
- Taking Common Cause failure into account for sensors of a channel.

The bottom of **Configuration of architecture** tab enables to define the configuration of sensor part. Possible choices are:

- The number of channels and the (logical) configuration between channels. (cf. **Configuration des canaux**)
- Number of actuators in each channel and the configuration of these components in the channel.
- For each actuator, the number of sub-actuators (0, 1, or 2), and the configuration of these sub-actuators.
- Taking Common Cause failure into account for all actuators. (cf. **Configuration des DCC**)
- Taking Common Cause failure into account for actuators and sub-actuator of the channel.
- Taking Common Cause failure into account for sub-actuators of the actuator.

3.2. Voting for components of a chanel

Usually, for each chanel, a MooN voting means that you need M components at threshold (detecting problem) to trip (put the system under control in a safe mode). For sensors, the SIL module distinguish MooNS (Safety) and MooNA(Availability) voting.

- **Vote with "A" type architecture** : the invalidity of the sensor triggers no action other than an alarm (availability). The solver logic is modified, excluding sensors with detected failure. In this case, we define a number (X) of detected failure from which the channel trips. This number (X) is fixed by default for TOTAL (but can be modified in M configuration):
  - 3 si plus de 3 composants
  - 3 si 3 composants
  - 2 si 2 composants
  - 1 si 1 composant

- **Vote with "S" type architecture** : the invalidity of the sensor triggers the safety system (Safe).

- **Vote with "M" type architecture**: It is exactly the same definition as type "A". But X (the number of detected failure leading to trip) can be modified by users.

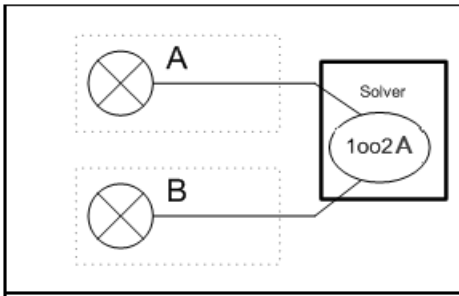
The reconfigurations in A/M configuration are the following:

- 1oo3 -> 1oo2 -> 1oo1
- 2oo3 -> 1oo2 -> 1oo1
- 3oo3 -> 2oo2 -> 1oo1
- MooN -> Moo(N-1)-> Moo(N-2) etc while N-i > M, then M and N are decreased of 1 until 2oo3 configuration
- NooN -> (N-1)oo(N-1) etc until 1oo1

Example: 4oo8 -> 4oo7 -> 4oo6 -> 4oo5 -> 3oo4 -> 2oo3

Following chapters detail S and A configuration for 1oo2 and 2oo3.

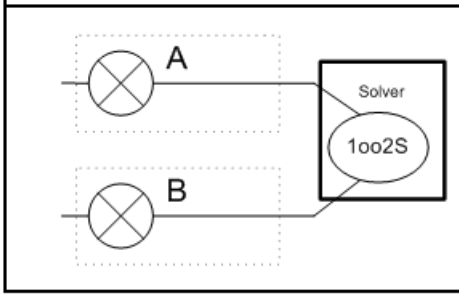
3.2.1. 1oo2S and 1oo2A



Sensor in 1oo2A configuration

Normal: The safety function is inactive
Tripped: The safety function is active

B\A	Normal	At threshold	Invalid
Normal	***Normal***	*Tripped*	***Normal***
At threshold	*Tripped*	*Tripped*	*Tripped*
Invalid	***Normal***	*Tripped*	*Tripped*

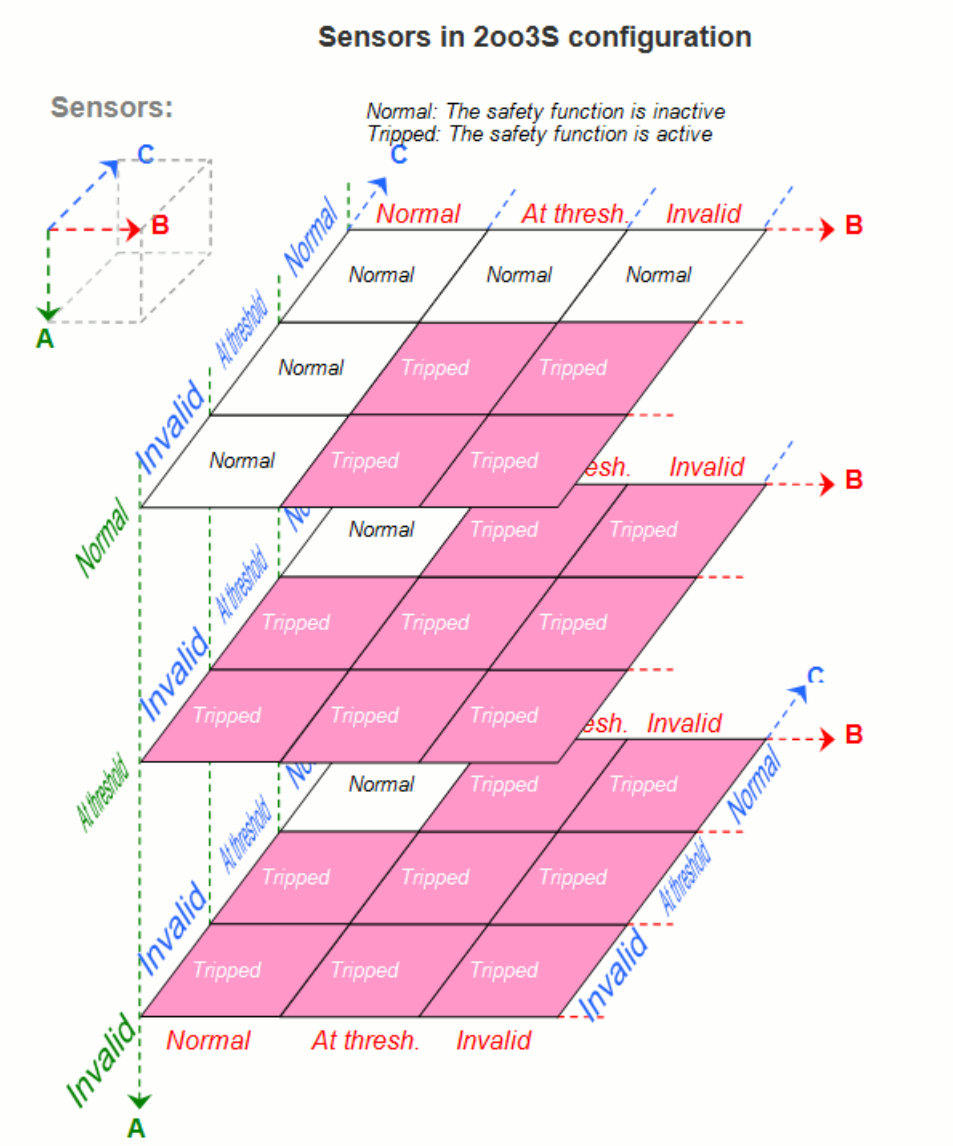


Sensor in 1oo2S configuration

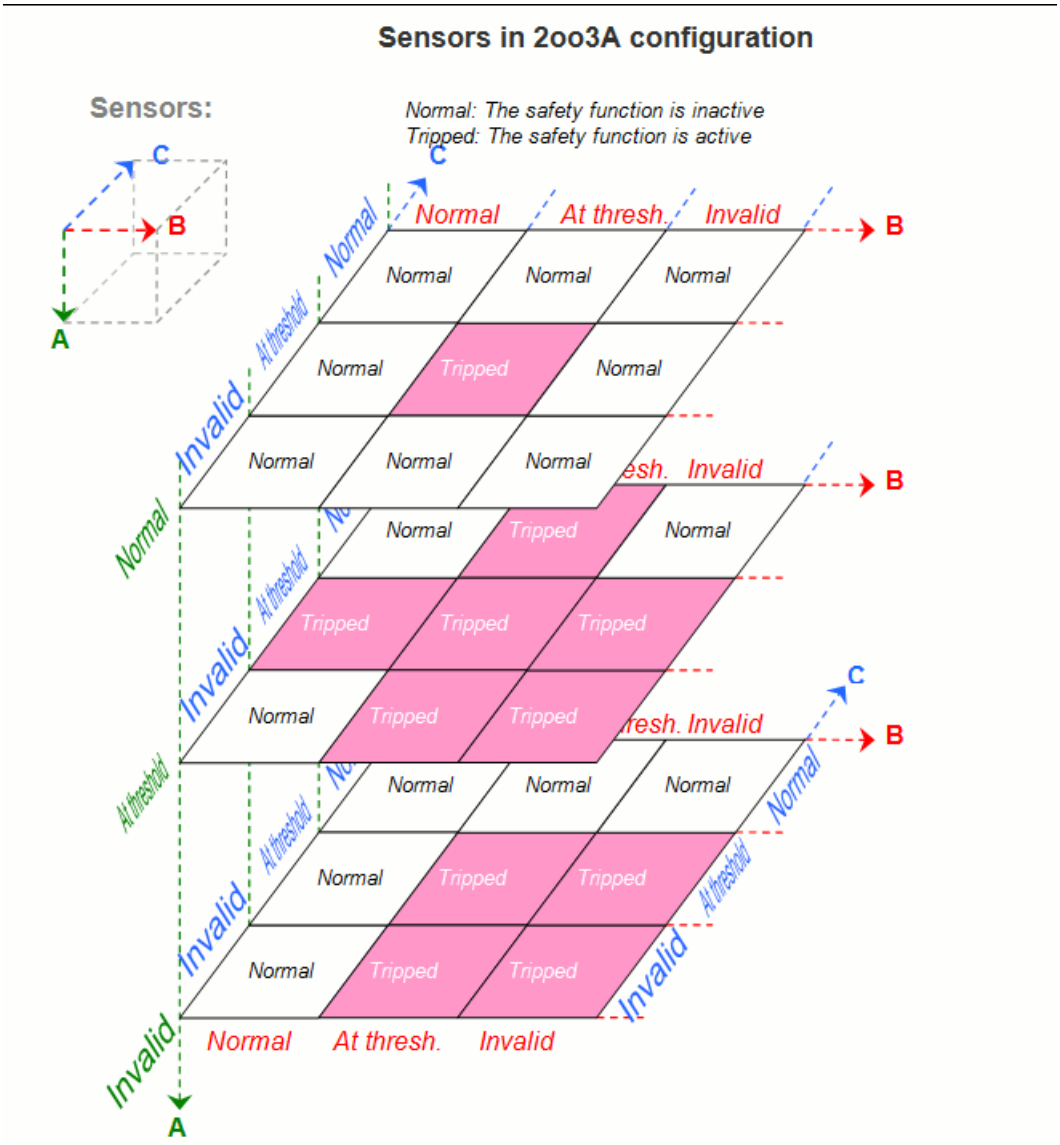
Normal: The safety function is inactive
Tripped: The safety function is active

B \ A	Normal	At threshold	Invalid
Normal	***Normal***	*Tripped*	*Tripped*
At threshold	*Tripped*	*Tripped*	*Tripped*
Invalid	*Tripped*	*Tripped*	*Tripped*

3.2.2. 2oo3S


Sensors in 2oo3S configuration
Sensors:
Normal: The safety function is inactive
Tripped: The safety function is active
A
B
C
Normal
At thresh.
Invalid
Tripped

3.2.3. 2oo3A



3.3. Configuration of channels of a part

You can select a MooN (M ou of N) configuration, in this case, the system needs M working sub-systems (out of N) to be available for its safety function. You can also choose a specific configuration. For example, if you need to configure 3 channels as follows: channel1 OR (channel2 AND channel3), select the **manual** button and type: **(1 | (2 & 3))** in the text field. In formula, each channel is remplaced by its number. For logical OR, use pipe (|) character. For AND use &. Operators have different priority, you must use parenthesis.

3.4. Take Common Cause Failures into account

You can use Common Cause Failures (CCF) at different levels of architecture. For each level, you can specify a beta-factor. For expert-users, you can display the DDC period configuration (with **Tools**), it let you specify a period (in hour) for DCC test. This period is automatically calculated. Uncheck the period checkbox if and only if you really know what you do.

4. Configuration of components

The aim is to specify values for each element of the SIF being studied.

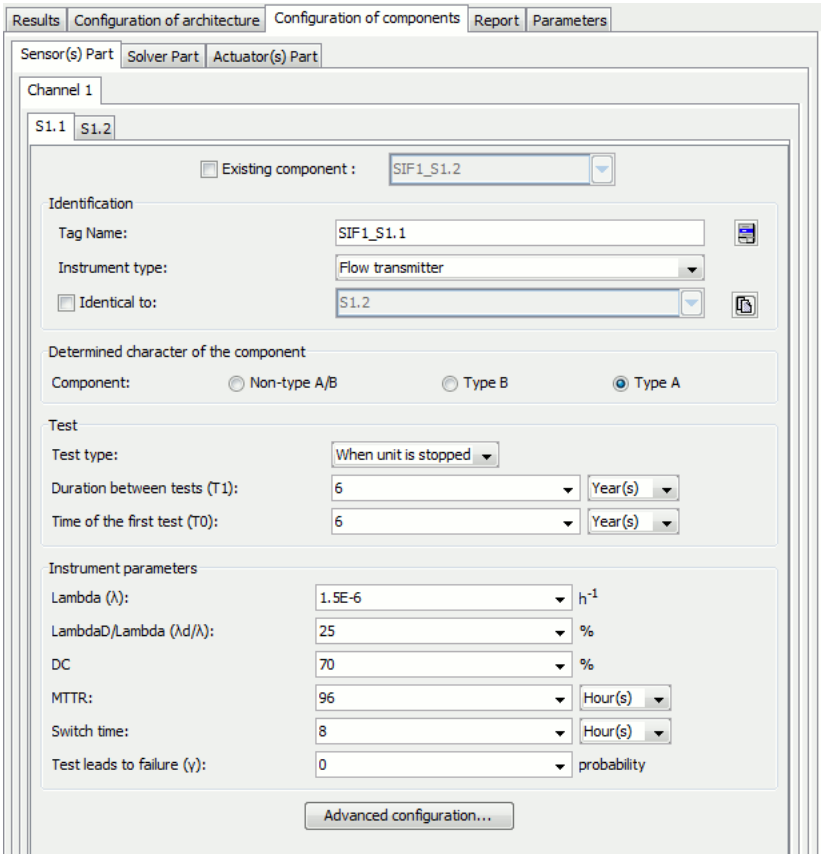
Do this with the tabs of configuration window :

- The **Sensor(s)** tab is used to configure the sensors,
- the **Solver** tab is used to configure the solver,
- the **Actuator(s)** tab is used to configure the actuators
- and the **Parameters** tab contains the definitions of the model's parameters.

NB: In the following chapters, all the numerical values entered can be real numbers, where the decimal separator is a dot. It is possible to write them as such: 0.0000015 or in scientific notation: 1.5E-6

4.1. Configuring the sensors

The sensors of the safety loop can be configured in the **Configuration of components**/**Sensor(s) Part** tab. Each sensor can be accessed separately in the sub-tabs **S1.1**, **S1.2**, etc. The first number (before the dot) is the channel number, the second (after the dot) is the position in the channel.



In the following paragraph, "the component" means the sensor.

The component may be already used/defined somewhere else in the system. In this case we speak about **existing component**. For example, when a component is in 2 chanels. The **existing component** can be selected in a list. It can be a component of the current SIF, of one of another SIF. This options is only available when you have many components of the same type.

If the component is not already used/defined, it must be defines. The following parameters can be configured.

- **Tag** : component's instrument tag on PID (e.g.: 10 PT 2034 for a sensor, or 10 UV 2034 for an actuator).
- **Instrument type** : type of instrument used. It is selected from a drop-down menu.
- **Identical to** : used to specify whether the component is identical to another component of the same type (i.e. a sensor when editing a sensor, another main actuator when editing a main actuator or another sub-actuator when editing a sub-actuator). It is different from **Existing component**. Here the component is not exactly the selected one, they are physically distinct, but they have same parameters. This functionality can only be accessed when the SIF comprises several components of the same type. If the checkbox is checked, only the **Tag** and **Instrument type** characteristics of the component can be edited (the others are identical to the reference component).
- **Copy another component's parameters** : enables you to copy the parameters of another component of the same type. This functionality can only be accessed when the SIF comprises several components of the same type. Only the characteristics **Tag** and **Identical to** are not copied. The components available are the same as those displayed for the functionality **Identical to**.
- **Modify the default parameters of the application** : enables you to manage the default parameters of the application and the document model system. Four actions can be chosen from the drop-down menu, displayed with a left click on the button:
  - **Save as default model** Save as default model. : saves the component's characteristics in the default model.
  - **Re-intialyse to default values** Re-initialyse to default values. : copies into the component the characteristics stored in the default model.
  - **Save in a model file** Save in a model-file ... : saves the component's characteristics in a model file, whose location must be specified. This file can be reused or sent to another person.
  - **Use a model** Use a model ... : copies into the component the characteristics stored in a model whose location must be specified.

- **Determined character of the component** : enables you to specify the component's determined character. The component is characterised by one of the three characters available :
  - **Non-type A/B** : indicates that the component is operating in negative safety mode (energise to trip) and without self-diagnostic system. Corresponds to the NS type (Non-safety component) of versions previous to 2013.
  - **Type B** : indicates that the component is operating in positive safety mode (fail-safe) or equipped with a self-diagnostic system. Corresponds to the S type (Standard component) of versions previous to 2013.
  - **Type A** : indicates that the component is operating in positive safety mode (fail-safe) and proven in use (or certified) and equipped with a self-diagnostic system (or implementation of several proof test) and access protected safeguarding the settings of the internal configuration parameters. Corresponds to the F type (Field proven component) of versions previous to 2013.

- **Test type** : enables you to specify the type of test used for the component. Two types of test can be selected from the drop-down menu:
  - **Test when unit is stopped** : means that the component is tested when the unit is stopped. The test does not harm the safety function as the unit is no longer working.
  - **Test when unit is working** : means that the component is tested when the unit is working. The component is no longer available to carry out its function and this affects the safety function. This can be used when a sensor has been by-passed to be tested and the installation has not been stopped.

  Remark: it is also possible to specify that the component will undergo no periodic test.
- **Duration between tests (T1)** : period of time between two proof tests of the component. The time unit is selected from a drop-down list (**hours**, **days**, **months**, **years**). The value of the duration can be edited manually or selected from a drop-down list displaying all of the parameters with a Time dimension (the model's parameters can be edited in the **Parameters** tab).
- **Time of the first test (T0)** : time at which the first test of the component is carried out. The modes for editing this characteristic (value and unit) are the same as for the duration between tests.

- **Lambda** λ : failure rate of the component (h^{-1}). This value can be edited manually or selected from a drop-down list displaying all of the parameters with a **Rate** dimension.

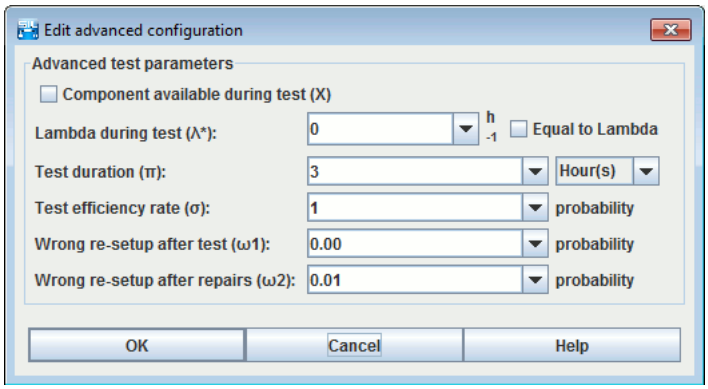
- **LambdaD/Lambda (λd/λ)** : proportion of dangerous failures among the total number of failures. This value can be edited manually or selected from a drop-down list displaying all of the parameters with a **Factor** dimension.
- **DC** : on-line diagnostic coverage and is a rate between 0 and 100%. A 0% rate means that no revealed failure can be detected. This value can be edited manually or selected from a drop-down list displaying all of the parameters with a **Factor** dimension.
- **MTTR (Mean Time To Repair) in h** : mean time between detection of a failure and the repair of the component . The time unit is selected from a drop-down list (**hours**, **days**, **months**, **years**). The value of the duration can be edited manually or selected from a drop-down list displaying all of the parameters with a **Time** dimension.

  Note: This field is editable only if **DC** is not 0 or if **Test type** is equal to **Test when unit is working**.
- **Switch time parameter** : is the period of time during which the component causing the failure is disconnected from the system and replaced by a component in working order. This time is necessarily lower than the MMTR.

  Note: This field is editable only if **LambdaD/Lambda** is not 1.
- **Test leads to failureγ (Gamma)** : probability [0,1] that the test will cause the hardware to fail. 0 means no test causes any failure, 1 mean every test causes failures. This value can be edited manually or selected from a drop-down list displaying all of the parameters with a **Probability** dimension.

  Note: This field is editable only if **DC** is not 0 or if **Test type** is not **Not tested**.

The advanced parameters of a sensor can be specified by left clicking on the **Advanced configuration button**.



The advanced parameters of the sensor are as follows:

- **Component available during test (X)** : specifies whether the component is able to carry out its safety mission during the test (if the checkbox is checked).
- **Safe failure repairs don't impact safety function** : It means (if checked) that repairs of safe failure haven't any impact on the safety function. Note: This field is editable only if **LambdaD/Lambda** < 100
- **Lambda during test λ*** : failure rate of the component during the tes (h^{-1}). The test conditions may cause extra stress and increase the lambda. This value can be edited manually or selected from a drop-down list displaying all of the parameters with a Rate dimension. It is possible to indicate that the value is to be equal to lambda (λ_{du}).
- **Test duration π (Pi)** : period of time necessary for testing the component. The time unit is selected from a drop-down list (**hours**, **days**, **months**, **years**). The value of the duration can be edited manually or selected from a drop-down list displaying all of the parameters with a Time dimension.

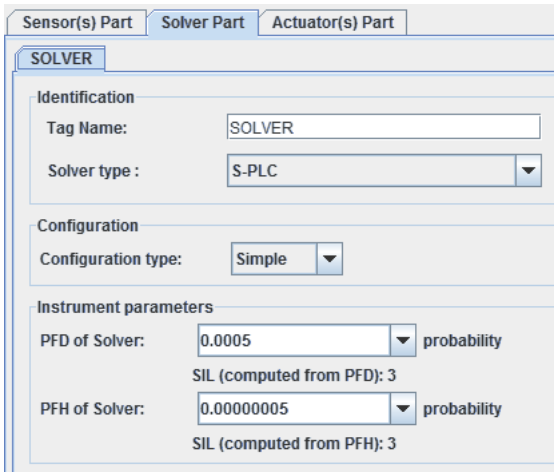
  Note: This field is editable only if **Test type** is equal to **Test when unit is working**.
- **Test efficiency rate σ (Sigma)** : cover or efficiency rate of the test. The value ranges from 0 (the test never detects anything) to 1(the test always detects the failure). This value can be edited manually or selected from a drop-down list displaying all of the parameters with a Probability dimension.
- **Wrong re-setup after testsω1 (Omega1)** : probability [0,1] of wrong re-setup of the equipment after the test. It is the probability that the component will not be able to carry out its safety mission after being tested by the operator. It can be left at 0 if you consider that the operators and test procedures are infallible (no omission of

a by-passed sensor, powering up the motor, etc.). This value can be edited manually or selected from a drop-down list displaying all of the parameters with a Probability dimension.

- **Wrong re-setup after repairsω2 (Omega2)** : probability [0,1] of wrong re-setup of the equipment after the repairs. It is the probability that the component will not be able to carry out its safety mission after being repaired (or changed) by the operator. It can be left at 0 if you consider that the operators and repairs procedures are infallible (powering up the new motor, etc.). This value can be edited manually or selected from a drop-down list displaying all of the parameters with a Probability dimension.

4.2. Configuring the solver

The solver of the safety loop can be configured in the **Solver** tab.



The solver may be used in many SIF, and may has been defined in an **existing solver** of the document. The reference-solver can be selected in a list. This options is only available when you have many SIF.

The solver is configured using the following parameters:

- **Tag** : solver's instrument tag on PID (e.g.: 10 ESD 06).
- **Solver type** : type of solver used. It is selected from a drop-down menu.

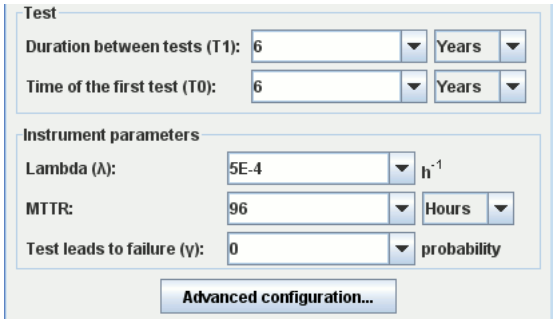
- **Configuration type** : specifies the solver's configuration type. Two types of configuration can be selected from the drop-down menu:
  - **Simple** : the solver is modelled by a constant law.
  - **Advanced** : the solver is modelled by a full periodic test law.

The parameters of the solver are described under **Instrument parameters**. They depend on the type of configuration which has been selected.

In the case of a simple configuration, the parameters are as follows:

- **PFD of solver** : probability that the solver will not work when triggered. This value can be edited manually or selected from a drop-down list displaying all of the parameters with a **Probability** dimension.
- **SIL (computed from PFD)** : automatically displays the solver's SIL computed based on the solver's PFD.
- **PFH of solver** : the PFH of the solver, given by manufacturer or by experience feedbacks.
- **SIL (computed from PFH)** : automatically displays the solver's SIL computed based on the solver's PFH.

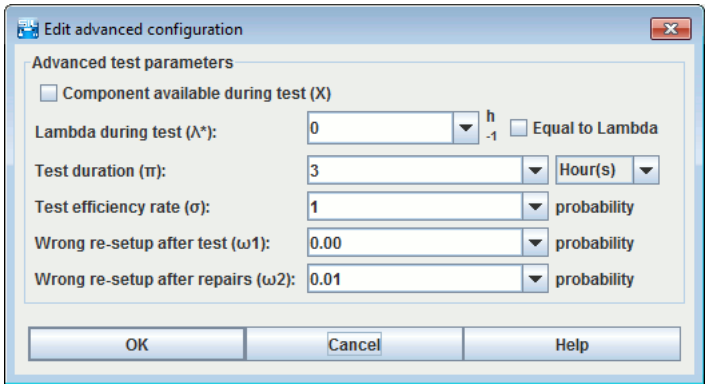
In the case of an advanced configuration, the parameters are as follows:



- **Duration between tests (T1)** : period of time between two proof tests of the component. The time unit is selected from a drop-down list (**hours**, **days**, **months**, **years**). The value of the duration can be edited manually or selected from a drop-down list displaying all of the parameters with a Time dimension (the model's parameters can be edited in the **Parameters** tab).
- **Time of the first test (T0)** : time at which the first test of the component is carried out. The modes for editing this characteristic (value and unit) are the same as for the duration between tests.

- **Lambda** λ : failure rate of the component (h^{-1}). This value can be edited manually or selected from a drop-down list displaying all of the parameters with a **Rate** dimension.
- **MTTR (Mean Time To Repair) in h** : mean time between detection of a failure and the repair of the component . The time unit is selected from a drop-down list (**hours**, **days**, **months**, **years**). The value of the duration can be edited manually or selected from a drop-down list displaying all of the parameters with a **Time** dimension.
- **Test leads to failure**γ **(Gamma)** : probability [0,1] that the test will cause the hardware to fail. 0 means no test causes any failure, 1 mean every test causes failures. This value can be edited manually or selected from a drop-down list displaying all of the parameters with a **Probability** dimension.

Other parameters can be accessed by left clicking on the **Advanced configuration ...** button (only for a solver configured in advanced mode).



- **Component available during test (X)** : specifies whether the component is able to carry out its safety mission during the test (if the checkbox is checked).
- **Safe failure repairs don't impact safety function** : It means (if checked) that repairs of safe failure haven't any impact on the safety function. Note: This field is editable only if **LambdaD/Lambda** < 100
- **Lambda during test** λ***** : failure rate of the component during the tes (h^{-1}). The test conditions may cause extra stress and increase the lambda. This value can be edited manually or selected from a drop-down list displaying all of the parameters with a Rate dimension. It is possible to indicate that the value is to be equal to lambda (λ_{du}).
- **Test duration** π **(Pi)** : period of time necessary for testing the component. The time unit is selected from a drop-down list (**hours**, **days**, **months**, **years**). The value of the duration can be edited manually or selected from a drop-down list displaying all of the parameters with a Time dimension.

Note: This field is editable only if **Test type** is equal to **Test when unit is working**.

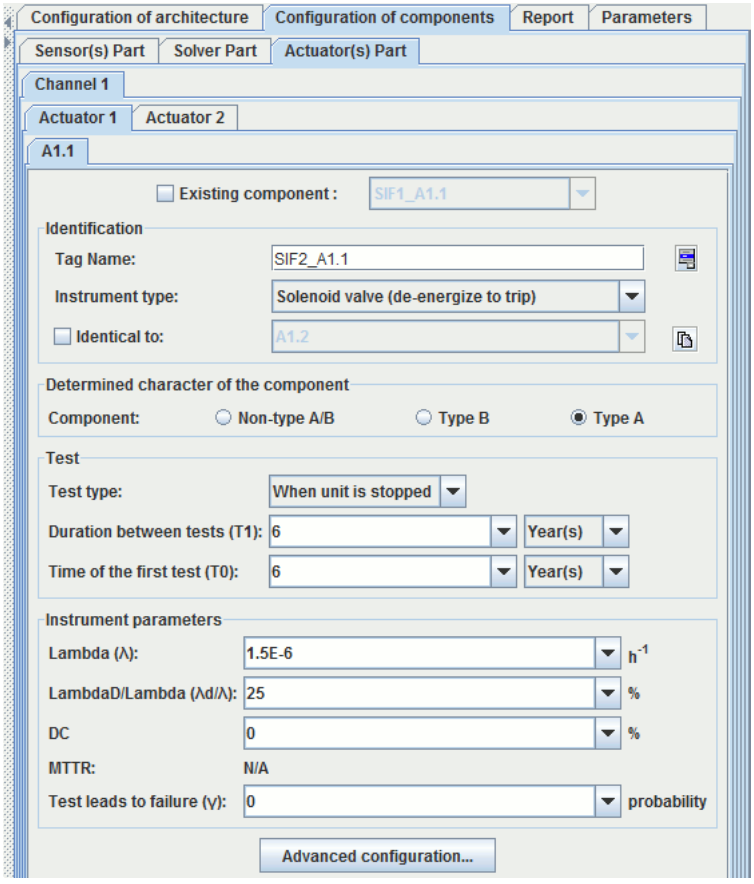
- **Test efficiency rate σ (Sigma)** : cover or efficiency rate of the test. The value ranges from 0 (the test never detects anything) to 1(the test always detects the failure). This value can be edited manually or selected from a drop-down list displaying all of the parameters with a Probability dimension.
- **Wrong re-setup after testsω1 (Omega1)** : probability [0,1] of wrong re-setup of the equipment after the test. It is the probability that the component will not be able to carry out its safety mission after being tested by the operator. It can be left at 0 if you consider that the operators and test procedures are infallible (no omission of a by-passed sensor, powering up the motor, etc.). This value can be edited manually or selected from a drop-down list displaying all of the parameters with a Probability dimension.
- **Wrong re-setup after repairsω2 (Omega2)** : probability [0,1] of wrong re-setup of the equipment after the repairs. It is the probability that the component will not be able to carry out its safety mission after being repaired (or changed) by the operator. It can be left at 0 if you consider that the operators and repairs procedures are infallible (powering up the new motor, etc.). This value can be edited manually or selected from a drop-down list displaying all of the parameters with a Probability dimension.

4.3. Configuring the actuators

The actuators of the safety loop can be configured in the **Configuration of componentsActuator(s) Parts** tab. The actuators can be classified as follows:

- **Main actuators** : they have 0, 1 or 2 sub-actuators.
- **Sub-actuators** : they are set up in series with their respective actuators. The sub-actuators of a same main actuator are set up in series (2oo2) or parallel (1oo2).

Each main actuator can be accessed separately in the sub-tabs **A1.1**, **A1.2**, ..., and each sub-actuator in the sub-tabs **A1.1a**, **A1.1b**, ...



In the following paragraph, the actuator (main or sub) will be called "the component".

The component may be already used/defined somewhere else in the system. In this case we speak about **existing component**. For example, when a component is in 2 chanels. The **existing component** can be selected in a list. It can be a component of the current SIF, of one of another SIF. This options is only available when you have many components of the same type.

If the component is not already used/defined, it must be defines. The following parameters can be configured.

- **Tag** : component's instrument tag on PID (e.g.: 10 PT 2034 for a sensor, or 10 UV 2034 for an actuator).
- **Instrument type** : type of instrument used. It is selected from a drop-down menu.
- **Identical to** : used to specify whether the component is identical to another component of the same type (i.e. a sensor when editing a sensor, another main actuator when editing a main actuator or another sub-actuator when editing a sub-actuator). It is different from **Existing component**. Here the component is not exactly the selected one, they are physically distinct, but they have same parameters. This functionality can only be accessed when the SIF comprises several components of the same type. If the checkbox is checked, only the **Tag** and **Instrument type** characteristics of the component can be edited (the others are identical to the reference component).
- **Copy another component's parameters** : enables you to copy the parameters of another component of the same type. This functionality can only be accessed when the SIF comprises several components of the same type. Only the characteristics **Tag** and **Identical to** are not copied. The components available are the same as those displayed for the functionality **Identical to**.
- **Modify the default parameters of the application** : enables you to manage the default parameters of the application and the document model system. Four actions can be chosen from the drop-down menu, displayed with a left click on the button:
  - **Save as default model** Save as default model. : saves the component's characteristics in the default model.
  - **Re-intialyse to default values** Re-initialyse to default values. : copies into the component the characteristics stored in the default model.
  - **Save in a model file** Save in a model-file ... : saves the component's characteristics in a model file, whose location must be specified. This file can be reused or sent to another person.
  - **Use a model** Use a model ... : copies into the component the characteristics stored in a model whose location must be specified.

- **Determined character of the component** : enables you to specify the component's determined character. The component is characterised by one of the three characters available :
  - **Non-type A/B** : indicates that the component is operating in negative safety mode (energise to trip) and without self-diagnostic system. Corresponds to the NS type (Non-safety component) of versions previous to 2013.
  - **Type B** : indicates that the component is operating in positive safety mode (fail-safe) or equipped with a self-diagnostic system. Corresponds to the S type (Standard component) of versions previous to 2013.
  - **Type A** : indicates that the component is operating in positive safety mode (fail-safe) and proven in use (or certified) and equipped with a self-diagnostic system (or implementation of several proof test) and access protected safeguarding the settings of the internal configuration parameters. Corresponds to the F type (Field proven component) of versions previous to 2013.

- **Test type** : enables you to specify the type of test used for the component. Two types of test can be selected from the drop-down menu:
  - **Test when unit is stopped** : means that the component is tested when the unit is stopped. The test does not harm the safety function as the unit is no longer working.
  - **Test when unit is working** : means that the component is tested when the unit is working. The component is no longer available to carry out its function and this affects the safety function. This can be used when a sensor has been by-passed to be tested and the installation has not been stopped.

  Remark: it is also possible to specify that the component will undergo no periodic test.
- **Duration between tests (T1)** : period of time between two proof tests of the component. The time unit is selected from a drop-down list (**hours**, **days**, **months**, **years**). The value of the duration can be edited manually or selected from a drop-down list displaying all of the parameters with a Time dimension (the model's parameters can be edited in the **Parameters** tab).

- **Time of the first test (T0)** : time at which the first test of the component is carried out. The modes for editing this characteristic (value and unit) are the same as for the duration between tests.

- **Lambda** λ : failure rate of the component (h^{-1}). This value can be edited manually or selected from a drop-down list displaying all of the parameters with a **Rate** dimension.
- **LambdaD/Lambda (λd/λ)** : proportion of dangerous failures among the total number of failures. This value can be edited manually or selected from a drop-down list displaying all of the parameters with a **Factor** dimension.
- **DC** : on-line diagnostic coverage and is a rate between 0 and 100%. A 0% rate means that no revealed failure can be detected. This value can be edited manually or selected from a drop-down list displaying all of the parameters with a **Factor** dimension.
- **MTTR (Mean Time To Repair) in h** : mean time between detection of a failure and the repair of the component . The time unit is selected from a drop-down list (**hours**, **days**, **months**, **years**). The value of the duration can be edited manually or selected from a drop-down list displaying all of the parameters with a **Time** dimension.

  Note: This field is editable only if **DC** is not 0 or if **Test type** is equal to **Test when unit is working**.
- **Switch time parameter** : is the period of time during which the component causing the failure is disconnected from the system and replaced by a component in working order. This time is necessarily lower than the MMTR.

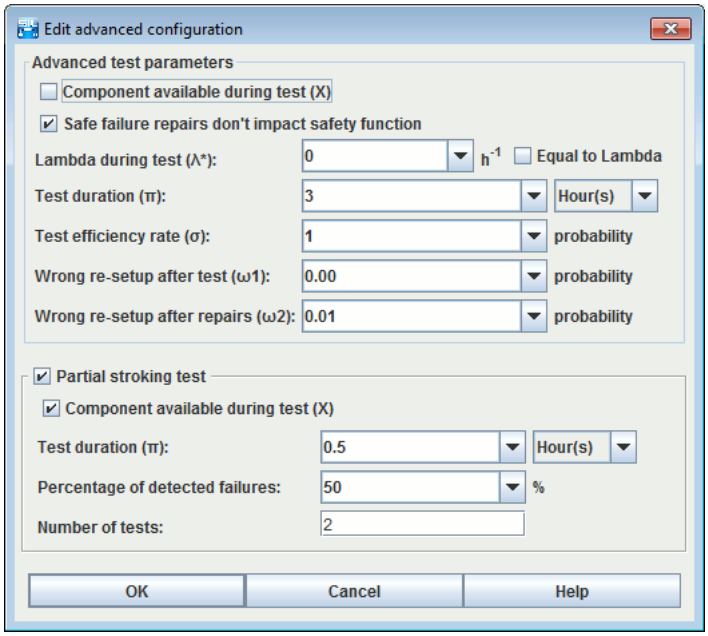
  Note: This field is editable only if **LambdaD/Lambda** is not 1.
- **Test leads to failureγ (Gamma)** : probability [0,1] that the test will cause the hardware to fail. 0 means no test causes any failure, 1 mean every test causes failures. This value can be edited manually or selected from a drop-down list displaying all of the parameters with a **Probability** dimension.

  Note: This field is editable only if **DC** is not 0 or if **Test type** is not **Not tested**.

Important

NB about Sub-actuators: Sub-actuators do not have a **Determined character of the component** characteristic. The section relating to this characteristic does therefore not appear when configuring the sub-actuators. As a rule, the sub-actuator has the same character as the one defined for its main actuator.

The advanced parameters of an actuator (main or sub) can be specified by left clicking on the **Advanced configuration** button.



The advanced parameters of the actuator are as follows:

- **Component available during test (X)** : specifies whether the component is able to carry out its safety mission during the test (if the checkbox is checked).

- **Safe failure repairs don't impact safety function** : It means (if checked) that repairs of safe failure haven't any impact on the safety function. Note: This field is editable only if **LambdaD/Lambda** < 100
- **Lambda during test λ*** : failure rate of the component during the tes (h^{-1}). The test conditions may cause extra stress and increase the lambda. This value can be edited manually or selected from a drop-down list displaying all of the parameters with a Rate dimension. It is possible to indicate that the value is to be equal to lambda (λ_{du}).
- **Test duration π (Pi)** : period of time necessary for testing the component. The time unit is selected from a drop-down list (**hours**, **days**, **months**, **years**). The value of the duration can be edited manually or selected from a drop-down list displaying all of the parameters with a Time dimension.

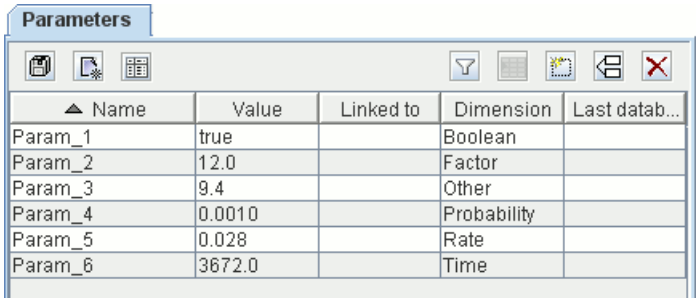
  Note: This field is editable only if **Test type** is equal to **Test when unit is working**.
- **Test efficiency rate σ (Sigma)** : cover or efficiency rate of the test. The value ranges from 0 (the test never detects anything) to 1(the test always detects the failure). This value can be edited manually or selected from a drop-down list displaying all of the parameters with a Probability dimension.
- **Wrong re-setup after testsω1 (Omega1)** : probability [0,1] of wrong re-setup of the equipment after the test. It is the probability that the component will not be able to carry out its safety mission after being tested by the operator. It can be left at 0 if you consider that the operators and test procedures are infallible (no omission of a by-passed sensor, powering up the motor, etc.). This value can be edited manually or selected from a drop-down list displaying all of the parameters with a Probability dimension.
- **Wrong re-setup after repairsω2 (Omega2)** : probability [0,1] of wrong re-setup of the equipment after the repairs. It is the probability that the component will not be able to carry out its safety mission after being repaired (or changed) by the operator. It can be left at 0 if you consider that the operators and repairs procedures are infallible (powering up the new motor, etc.). This value can be edited manually or selected from a drop-down list displaying all of the parameters with a Probability dimension.

- **With partial stroking test** : if checked, specifies whether the component takes partial stroking tests into account, as for example the partial stroke testing of a valve gate.
- **Efficiency of partial stroking tests** , **Proportion of detected failure** :proportion of hidden failures detected during partial stroking tests (0-100%). 0% means no failure is detected, 100% means every failure is detected. The value of the efficiency can be edited manually or selected from a drop-down list displaying all the parameters with a Factor dimension. This characteristic is accessible only if the component takes partial stroking tests into account.
- **Number of tests** : number of partial stroking tests carried out between two full tests.

NB: Sub-actuators do not take partial stroking tests into account. There is therefore no Partial stroking test section in the sub-actuator configuration tab.

4.4. Editing the parameters

The parameters table contains all of the model's parameters.



Each parameter is defined by the following:

- **Name** : the parameter's name (unique).
- **Value** : the parameter's value (consistent with its dimension).
- **Linked to** : the identifier of the database to which the parameter is linked.

- **Dimension** : the parameter's dimension. It is selected from a drop-down menu: Boolean, factor, probability, rate, time, other.
- **Last database** : last database used to update the parameter.

The parameters can then be used to fill in the characteristics of the safety loop's components.

This table can be accessed using the tabs situated on the right but can also be opened in another window via the menu **Data and Computations - Edit parameters**.

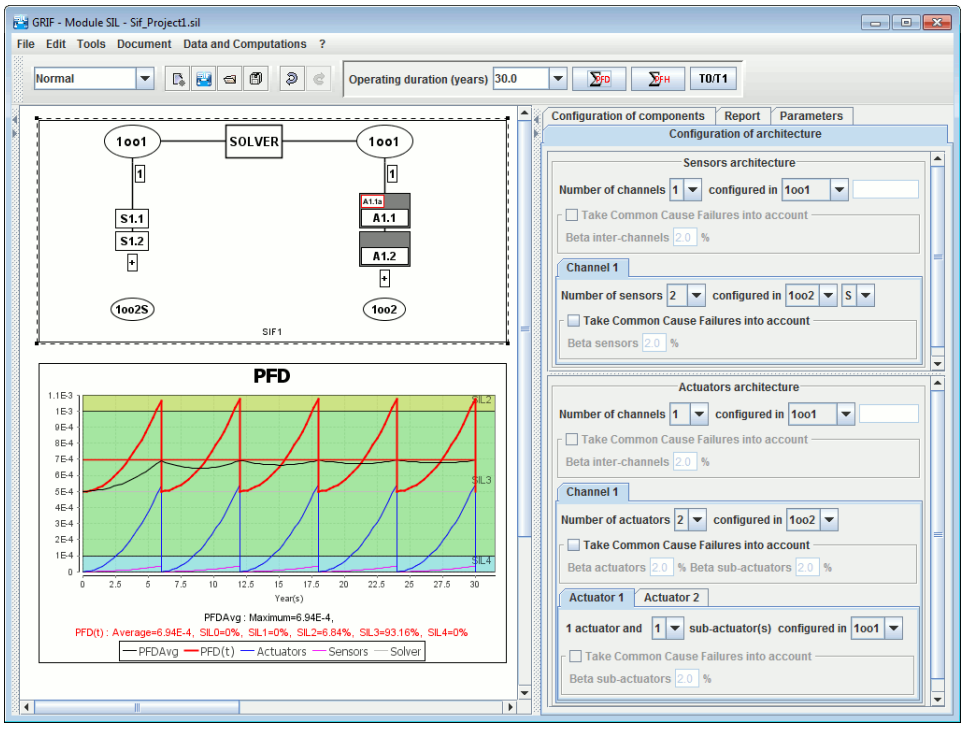
5. Computes

5.1. Launch PFD/PFH computation

When all of the components have been configured, computations can be started. PFD Computations are launched via the menu **Data and Computations/Launch PFD computations** or by clicking on the icon. PFH Computations are launched via the menu **Data and Computations/Launch PFH computations** or by clicking on the icon.

NB : if many SIF has been created, computation is done on each SIF.

The chart, which contained no information, has now been updated.



Reminder: The combination Control+Scroll wheel enables you to enlarge (zoom in) or reduce the window.

The x-axis represents the time in hours and the y-axis represents the probability of failure of the SIF when triggered, also called PFD. The chart ranges from 0 to 30 years by default but it is possible to modify this value as explained in the chapter on curves. There are 5 curves in the chart:

- **PFD(t) or PFH(t)** : the instantaneous value of the system's PFD/PFH.
- **PFD Avg or PFH** : the average value of the system's PFD/PFH.
- **Actuators** : the instantaneous value of the PFD/PFH of the actuator part of the system.
- **Sensors** : the instantaneous value of the PFD/PFH of the sensor part of the system.
- **Solver** : the instantaneous value of the solver's PFD/PFH.

The curves are located in one or several bands of color. These bands represent the PFD ranges, which define the SIL:

- **SIL 0** : instantaneous PFD $\in [10^{-1}; 1]$. instantaneous PFH $\in [10^{-5}; +\text{infinity}]$.
- **SIL 1** : instantaneous PFD $\in [10^{-2}; 10^{-1}[$. PFH instantanée $\in [10^{-6}; 10^{-5}[$.

- **SIL 2** : instantaneous PFD $\in [10^{-3}; 10^{-2}[$. instantaneous PFH $\in [10^{-7}; 10^{-6}[$.
- **SIL 3** : instantaneous PFD $\in [10^{-4}; 10^{-3}[$. instantaneous PFH $\in [10^{-8}; 10^{-7}[$.
- **SIL 4** : instantaneous PFD $\in [0; 10^{-4}[$. instantaneous PFH $\in [0; 10^{-8}[$.

6. Multi-loop systems

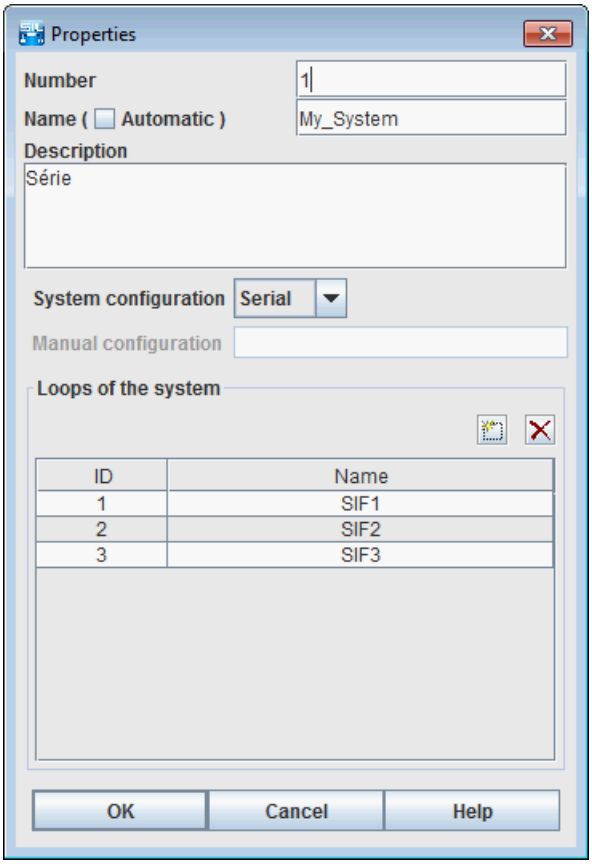
6.1. Presentation

When several loops (SIF) are created in a document, a **tree view** on left left become visible. The upper part let you browse the pages (one page by SIF). The lower part is for systems that are made with several loops.

6.2. Input

Double-click one the root of **Multi-loops systems** tree in order to create an empty system.

System editing can be done either with a double-click or with a right-click using **Properties** menu. The following window is displayed:



You can enter **Number** and a **Name**. The **Automatic** checkbox generates a name starting with a base name followed by the number.

A text area is available for adding a **Description** to your system.

The **System configuration** defines the logical use of the loops.

- **Serial** : Safety loops are in serial, every loop must be available to have an available system.
- **Parallel** : Safety loops are in Parallel boucles de sécurité sont en parallèle, le système reste disponible tant qu'il reste au moins une boucle disponible.
- **Manual** : You can specify the configuration of the system as 1 & (2 | 3), with 1,2 et 3 corresponding to the loops which ID is 1 2 and 3.

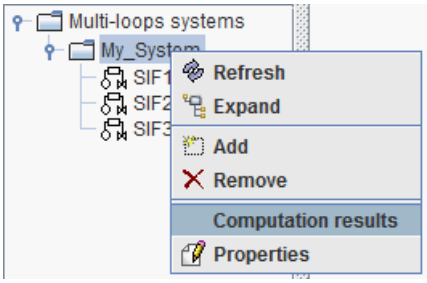
The **Loops of the system** part enables adding/removing/modifying of loops that are in the system.

6.3. Computations

System PFD/PFH computations are made as for SIF PFD/PFH computations. (Section 5.1, “Launch PFD/PFH computation”)

6.4. Reports and results

Results are available with a right-clic on the system, and then select **Computation results** in the menu.



The following window is displayed:

The **Description** part sum system configuration up.

The **For the system** part is used to specify the target values:

- **Requiered SIL** : value of the SIL that is requiered for the system.
- **Requiered RRF** : value of the RRF that is requiered for the system.

The **Computation** part displays computed values:

- **Operating duration** : the operating duration used for the computation.
- **PFD or PFH** : The computed PFDAvg or PFH.
- **Computed SIL** : SIL computed from PFD or PFH (architectural constraints are not taken into account).
- **Computed RRF** : RRF computed from PFD or PFH .

The **Results** part displayed achieved targets:

- **Achieved SIL** : Identical to computed SIL.
- **Conclusion of SIL for the system** : conclusion (compliant or not compliant).
- **Remark** : Remark generated by sofware.
- **Comments** : User comments.

The **Synthesis** part displays PFD/PFH curves of the system

6.5. PDF report and MS Excel report

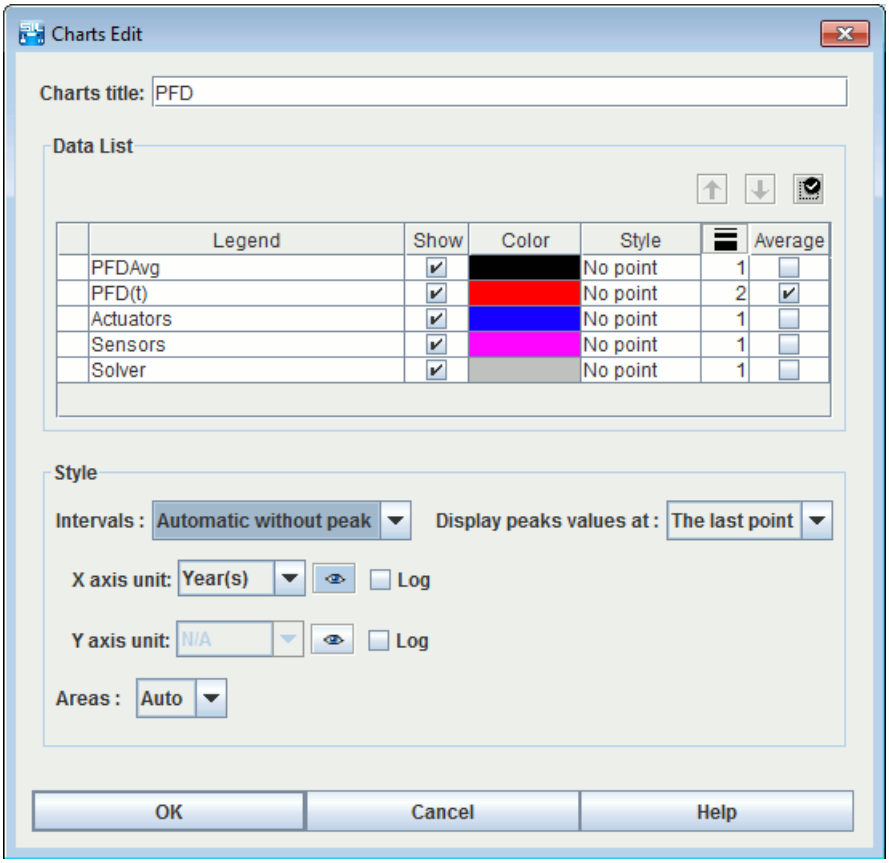
If there are system in your document, they will be automatically exported in reports. An additionnal section will be added for each system, at the end of the report. The system section contains informations in **Reports and results** window.

7. Charts

Curves are drawn to study the results better. Five curves are available : PFDAvg(t), $PFD_{System}(t)$, $PFD_{Actuators}(t)$, $PFD_{Solver}(t)$, $PFD_{Sensors}(t)$.

7.1. Charts Edit window

The Charts Edit window is displayed when user double-click on charts.



This window is divided into several parts:

1. **Charts Title**: allows you to give a title to the graphic.

2. **Data List**: This part contains a three-column table listing the chart's different curves (name, description, display, curve colour, curve style, curve thickness).Several buttons are available above this table.
   - **Up** : moves the selected curve upwards in the list.
   - **Down** : moves the selected curve downwards in the list.
   - **Save as default model** : saves current chart setting as default setting for new documents.

   For each curve, you can specify its colour, its style of points, its thickness and its display options.

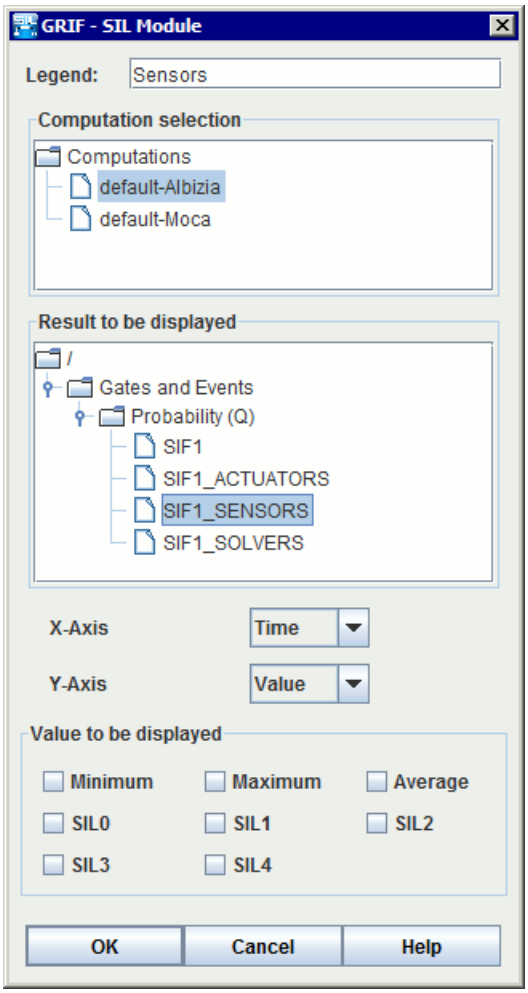
3. **Style**: This part deals with displaying curves.
   - **Style type**: specifies the type of all the chart's curves (line or histogram). N.B: For histogram style, bars going outside drawing zone will be drawn with a gradient to warn user that he has to change intervals to see the entire bar.
   - **Intervals on X and Y**: Specifies the display interval for the X and Y axes (default interval or user-defined interval). This last function can, for example, be used to zoom in on the most interesting parts of the curve.

The **log** check boxes are used to enable the logarithmic scale on the axis concerned. Important: 0 cannot be represented on a log scale, remember to give a strictly positive starting point (e.g.: E-10). If 0 is given, the log scale will start with an arbitrary value E-15.

When domain axe deals with time, you can choose time unit among : hours, days, months, years. Default display is "hours" because it is the usualy used unit for modeling. It's only available in SIL module.

7.2. Editing the curves

When a curve is edited (with a double-click on its name in list of curves), the curve edition window is displayed. The following window id displayed :



The window is divided into three parts:

- **Legends**: enables you to give a title to the curve.
- **Value to be displayed**: used to select the values which are to be displayed or not below the curve.

  For SIL curve (probability functions of times), available values are :
  - **SIL 0** : percentage of time spent in SIL 0.
  - **SIL 1** : percentage of time spent in SIL 1.
  - **SIL 2** : percentage of time spent in SIL 2.
  - **SIL 3** : percentage of time spent in SIL 3.
  - **SIL 4** : percentage of time spent in SIL 4.
  - **Minimum** : the minimum instantaneous PFD over the period studied.
  - **Maximum** : the maximum instantaneous PFD over the period studied.

- **Mean** : the average of the PFD over the period studied.

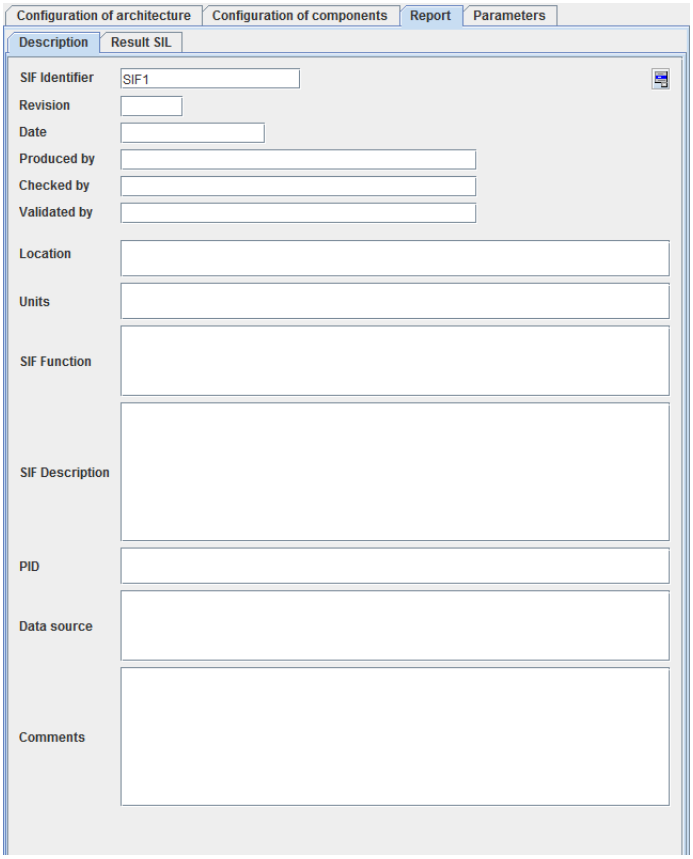
For average probability curves (like PFDAvg), available values are :
- **Minimum** : the minimum value of the average PFD over the period studied.
- **Maximum** : the maximum value of the average PFD over the period studied.
- **Mean** : the average value of the average PFD over the period studied (which is NOT the PFDAvg).

When the values are entered, just click on **OK** to close the windows.

8. Generating reports

8.1. Description

The PDF reports can be configured in the tab **Report** and its sub-tab **Description**:

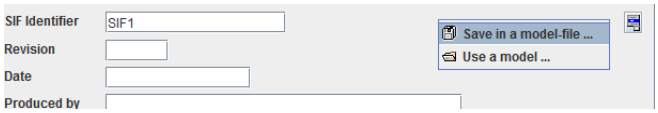


When report is generate the following fields are exported :

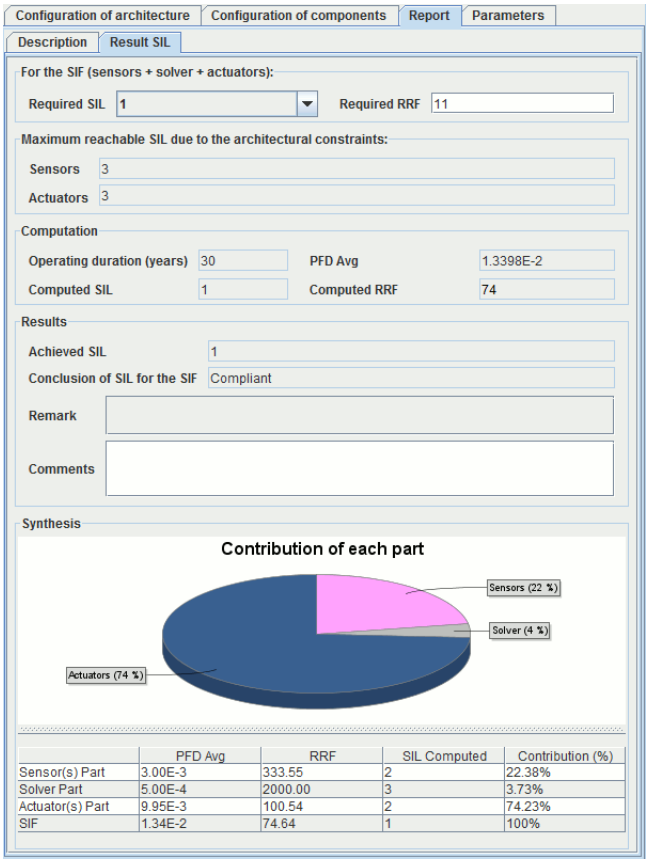
- **SIF Identifier** : identifier of the SIF or report.
- **Revision** : revision index of the report.
- **Date** : date on which the report was issued.
- **Produced by** : name of the author of the report.
- **Checked by** : name of the checker of the report.
- **Validated by** : name of the person who validated the report

- **Localization** : specify the refinery, the platform, the plant.
- **Units** : specify the units, the sectors, the workshops, the project.
- **SIF Function** : function of the SIF (top event).
- **Description of the SIF** : description of the SIF.
- **PID** : number of the PID.
- **Data source** : source of the data used in the computations (e.g.: TOTAL, EXIDA, OREDA, etc.).
- **Comments** : comments.

You can save fields of SIF in a model in order to use it for other SIF description. Click on the top right button:



8.2. Result SIL



Result SIL tab do a synthesis of results. On the top of the tab you must specify the objectives to be reached :

- **Required SIL** : value of the SIL required for the SIF.
- **Required RRF** : value of the RRF required for the SIF.

Then the softwre reminds you the maximum reachable SIL of each part. (not available if many channels)

- **Maximum reachable SIL for sensors** : maximum SIL which can be reached by the sensors due to architectural constraints.
- **Maximum reachable SIL for actuators** : maximum SIL which can be reached by the actuators due to architectural constraints.

The "Computation" part reminds the computed values

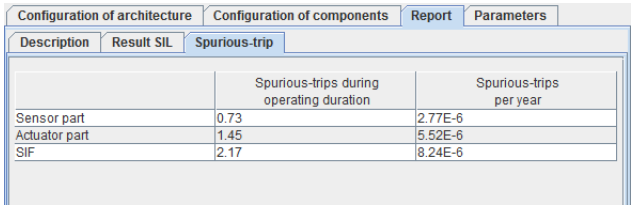
- **Operation duration** : The duration used to do computation.
- **PFD or PFH** : computed PFDAvg or PFH.
- **Computed SIL** : SIL obtained with computed PFD or PFH. Architectural contraints are not taken into account.
- **RRF Calculé** : RRF obtained with computed PFD or PFH.

Then the results part says if objectives are reached or not.

- **Achieved SIL** : SIL obtained for the SIF according to the PFD computation and architectural constraints.
- **Conclusion of SIL for the SIF** : conclusion (compliant or non-compliant).
- **Remark** : Remark generated by the software. It shows the part whose Max-SIL is limiting.
- **Comments** : Comments made by user.

At the end of the tab, a table shows you values for each part in order to identify the most important contributor.

8.3. Spurious-trip



When a sensors has a detected failure, it can lead to the triggering of safety function, even if it is not necessary. It's the same thing for safe failure of actuators, which trigger the safety function. That is why the MooN configuration (whith M > 1) are used, the triggering will not be made at the first safe failure.

The SIL module computes the number of expected spurious trips on a given architecture. **Spurious-trip** tab displays computation results of spurious-trips.

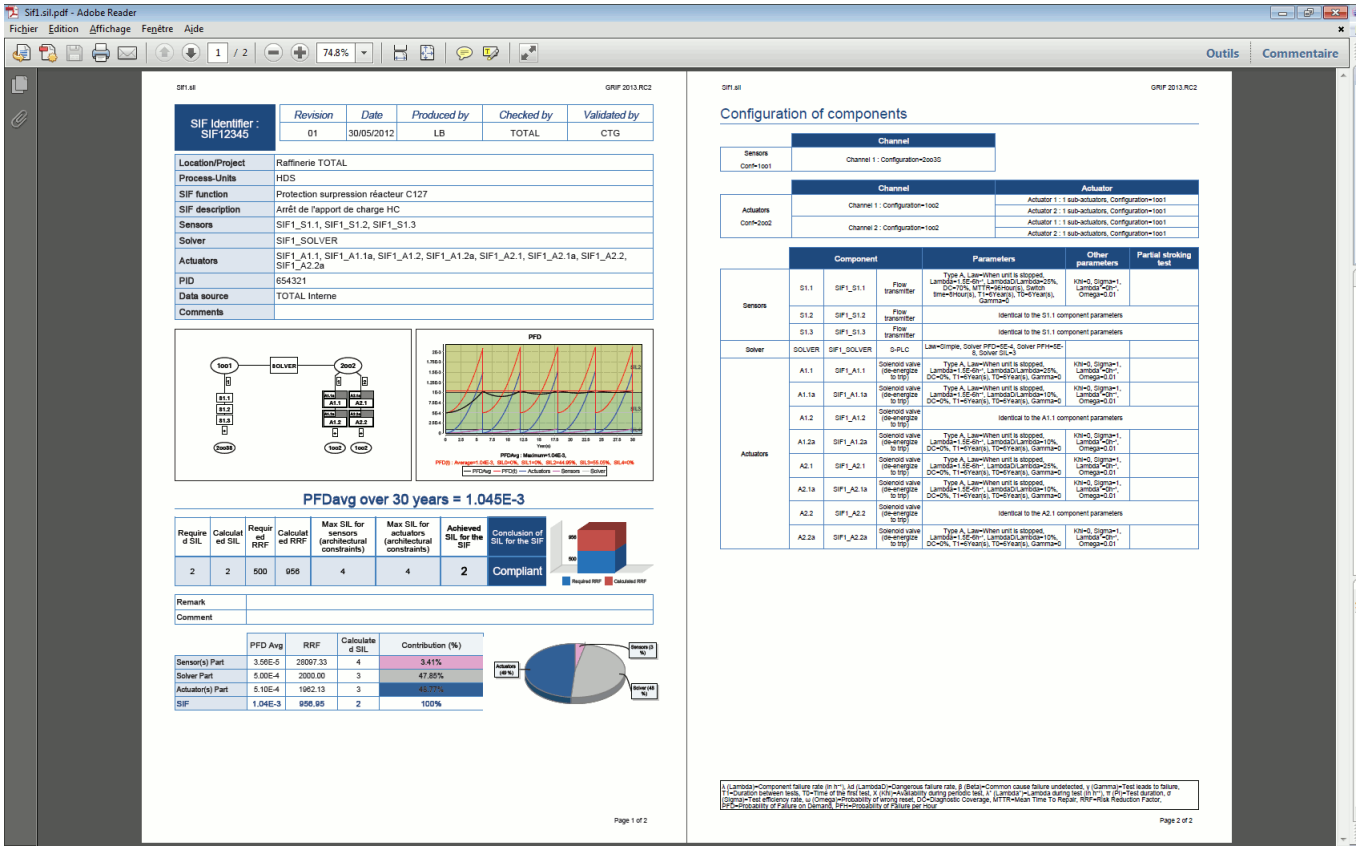
The export of spurious-trip-computation-results in reports is optional. Make sure that the **Spurious-trip in reports** option is selected in Application Options / Options.

8.4. PDF reports

When all the computations have been carried out, a report can be generated. The language of the report (English or French) can be selected.

the PDF report is generated from the menu **File/Create a report/PDF report (en)** (report written in English) or from the menu **File/Create a report/PDF report (fr)** (report written in French). In all two cases, you must select the location where the PDF file is to be stored and click on save. When the report is generated, it is opened with the programme associated with the PDF format (generally Acrobat Reader).

PDF report:


Sif1.sil.pdf - Adobe Reader
Fichier Edition Affichage Fenêtre Aide
Outils Commentaire
SIF Identifier : SIF12345
Revision 01
Date 30/05/2012
Produced by LB
Checked by TOTAL
Validated by CTG
Location/Project Raffinerie TOTAL
Process-Units HDS
SIF function Protection surpression réacteur C127
SIF description Arrêt de l'apport de charge HC
Sensors SIF1_S1.1, SIF1_S1.2, SIF1_S1.3
Solver SIF1_SOLVER
Actuators SIF1_A1.1, SIF1_A1.1a, SIF1_A1.2, SIF1_A1.2a, SIF1_A2.1, SIF1_A2.1a, SIF1_A2.2, SIF1_A2.2a
PID 654321
Data source TOTAL Interne
Comments
PFDavg over 30 years = 1.045E-3
Required SIL 2
Calculated SIL 2
Required RRF 500
Calculated RRF 958
Max SIL for sensors (architectural constraints) 4
Max SIL for actuators (architectural constraints) 4
Achieved SIL for the SIF 2
Conclusion of SIL for the SIF Compliant
Remark
Comment
Sensor(s) Part 3.56E-5 28097.33 4 3.41%
Solver Part 5.00E-4 2000.00 3 47.85%
Actuator(s) Part 5.10E-4 1962.13 3 48.73%
SIF 1.04E-3 956.95 2 100%
Configuration of components
Page 1 of 2
Page 2 of 2

8.5. Mirosoft Excel XLSX file format export

You can also export to XLSX format thanks to **File** menu. The file is made of two tabs, the first one for SIF description and results, the second one for configuration of components.

9. Glossary

9.1. Format

All values can be entered in two different ways:

- **"Normal" notation** : the decimal separator is the dot, e.g. 0.0000015.
- **Scientific notation** : the decimal separator is the dot, e.g. 1.5E-6 which corresponds to 0.0000015.

9.2. Definition and explanation of the acronyms and parameters

- **Beta (β)** : proportion of common cause failures (in %).
- **CCF or DCC** : Common Cause Failure. When several identical elements are put in a system, there is always a probability that they will fail at the same time from a common cause (design problem, external phenomena for example). This is called a common cause failure.
- **Component available during test (X)** : specifies whether the component is able to carry out its safety mission during the test (if the checkbox is checked).
- **DC** : on-line diagnostic coverage and is a rate between 0 and 100%. A 0% rate means that no revealed failure can be detected.
- **Detected** : applies to the equipment and means detected by diagnostic tests, periodic tests or human intervention (e.g. physical inspection and manual tests) or during normal operation.
- **DCS** : Distributed Control System
- **Determinate** : A component can be one of these 3 types : "Non-type A/B", "Type A" or "Type B"
- **Duration between tests (T1)** : period of time between two proof tests of the component.
- **E/E/PE** : electrical/electronic/ programmable electronic. Technology based on electricity (E), and/or electronics (E) and/or programmable electronics (EP). NB. - This term designates all devices which work according to electrical principles.
- **Efficiency of partial stroking tests** , **Proportion of detected failure** :proportion of hidden failures detected during partial stroking tests (0-100%). 0% means no failure is detected, 100% means every failure is detected.
- **Failure** : a functional unit ceases to accomplish its required function.
- **Lambda** λ : failure rate of the component (h^{-1}).
- **Lambda during test λ*** : failure rate of the component during the tes (h^{-1}). The test conditions may cause extra stress and increase the lambda.
- **Lambda D (λ d)** : dangerous failures. Failure with the potential to put the safety system into a dangerous state or make it unable to carry out its function.
- **MDT (in h)** : indicates the mean time between the occurrence of a failure and the re-start of the system (Mean Down Time). It is the average downtime.
- **MTTF (in h)** : indicates the mean time between the start-up of the system and the occurrence of the first failure (Mean Time To Failure). It is the average time of operation before the first failure occurs. λ = 1/ MTTF for a component.
- **MTTR (Mean Time To Repair) in h** : mean time between detection of a failure and the repair of the component .
- **Non-detected (Undetected)** : applies to the equipment and means non-detected by diagnostic tests, periodic tests or human intervention (e.g. physical inspection and manual tests) or during normal operation.
- **Number of tests** : number of partial stroking tests carried out between two full tests.
- **Operating duration (Years)** : means the foreseen operating industrial duration of the Safety Instrumented Function (SIF) installed on its process unit.
- **PFD** : Probability of Failure on Demand. Cf. Norm IEC61508. Can be defined as Unavailability
- **PFH** : Probability of Failure per Hour. Cf. Norm IEC61508. Can be defined as Unconditionnal Failure Intensity
- **Redundancy** : implementation in parallel of elements which have the same safety function so that the sub-system is more available.
- **Repair rate μ (Mu)** : repair rate in $^{-1}$, whose symbol is (μ). This value is equal to 1/MTTR, for a repair time of 48h, Mu = 1/48 = 2.08E-2

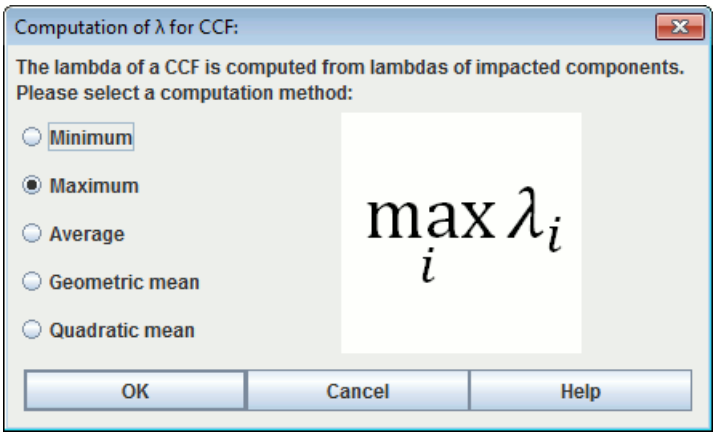
- **R.R.F** : Risk Reduction Factor of the SIF
- **Safety function** : function to be carried out by an E/E/EP safety system, by a safety system based on another technology or by an external risk reduction device, designed to ensure or maintain the controlled system in a safe state with regard to a specific dangerous event.
- **SIF** : Safety Instrumented Function.
- **SIL 0** : instantaneous PFD $\in [10^{-1}; 1]$. instantaneous PFH $\in [10^{-5}; +\text{infinity}]$.
- **SIL 1** : instantaneous PFD $\in [10^{-2}; 10^{-1}[$. PFH instantanée $\in [10^{-6}; 10^{-5}[$.
- **SIL 2** : instantaneous PFD $\in [10^{-3}; 10^{-2}[$. instantaneous PFH $\in [10^{-7}; 10^{-6}[$.
- **SIL 3** : instantaneous PFD $\in [10^{-4}; 10^{-3}[$. instantaneous PFH $\in [10^{-8}; 10^{-7}[$.
- **SIL 4** : instantaneous PFD $\in [0; 10^{-4}[$. instantaneous PFH $\in [0; 10^{-8}[$.
- **SIS** : Safety Instrumented System. Instrumented system used to carry out one or several safety functions. An SIS is made up of sensors, a logical processing system and actuators.
- **System** : set of elements which interact according to a specific model, an element, which may be another system called a sub-system. The sub-systems can themselves be either a command system or a controlled system made up of hardware, software and interacting with man.
- **S-PLC** : Safety-Programmable Logic Controller
- **Test duration π (Pi)** : period of time necessary for testing the component.
- **Test efficiency rate σ (Sigma)** : cover or efficiency rate of the test. The value ranges from 0 (the test never detects anything) to 1(the test always detects the failure).
- **Test leads to failureγ (Gamma)** : probability [0,1] that the test will cause the hardware to fail. 0 means no test causes any failure, 1 mean every test causes failures.
- **Test when unit is stopped** : means that the component is tested when the unit is stopped. The test does not harm the safety function as the unit is no longer working.
- **Test when unit is working** : means that the component is tested when the unit is working. The component is no longer available to carry out its function and this affects the safety function. This can be used when a sensor has been by-passed to be tested and the installation has not been stopped.
- **Time of the first test (T0)** : time at which the first test of the component is carried out.
- **Vote with "A" type architecture** : the invalidity of the sensor triggers no action other than an alarm (availability). The solver logic is modified, excluding sensors with detected failure. In this case, we define a number (X) of detected failure from which the channel trips. This number (X) is fixed by default for TOTAL (but can be modified in M configuration):
  - 3 si plus de 3 composants
  - 3 si 3 composants
  - 2 si 2 composants
  - 1 si 1 composant
- **Vote with "S" type architecture** : the invalidity of the sensor triggers the safety system (Safe).
- **Wrong re-setup after testsω1 (Omega1)** : probability [0,1] of wrong re-setup of the equipment after the test. It is the probability that the component will not be able to carry out its safety mission after being tested by the operator. It can be left at 0 if you consider that the operators and test procedures are infallible (no omission of a by-passed sensor, powering up the motor, etc.).
- **Oubli de reconfiguration après réparationω2 (Omega2)** : correspond à la probabilité [0,1] d'oubli de reconfiguration du matériel après la réparation (ou changement). Il s'agit de la probabilité que l'opérateur ne remette pas le composant dans l'état d'assurer sa mission de sécurité après la réparation. On peut la laisser à 0 si on estime que les opérateurs et les procédures de réparation sont infaillibles (Remise du moteur neuf sous tension, ...).

10. Appendix

10.1. Configuration of Lambda computation method for CCF

When using common cause failure, the software must compute a lambdaCCF that will be used for CCF. It is the one that will be multiplied by Beta. Assuming each component impacted bay a CCF has a different lambda, there are many methods to compute the lambdaCCF from the list of lambdas. Five methods are available :

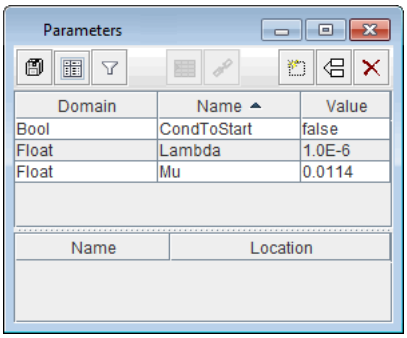
- Minimum: This method uses the minimum value of lambdas. Not recommanded.
- Maximum: Uses the maximum value of lambdas to be concervativ. This method was used in GRIF 2013 and previous version. It can be penalizing when lambda of components are very different.
- Average: This method uses the artimetic mean of lambdas.
- Geometric mean (PDS Method): This method uses the geometric mean of lambdas. It is PDS Method recommanded by SINTEF. It works fine with very different lambdas.
- Quadratic mean: This method uses the quadratic mean of lambdas.



10.2. Data Editing Tables

10.2.1. Description of the Tables

To create or modify data (parameters, variables, etc.), tables are available in the **Data and Computations menu** and in tabs at the right of the view. All the GRIF 2014 data tables operate in the same manner.



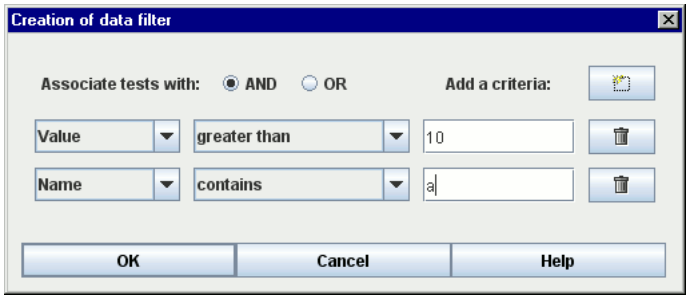
The data editing table/panel is divided into 3 parts:

- The top part containing the buttons.
- The main part containing the data table.

- The bottom part indicating what the selected data is used for.

	Saves the table in a text file.
	Opens the table in a text editor (that defined in the Options).
	Opens the column manager.
	When the **display selection** button is pressed, a click in the table leads to the selection in the input area.
	Displays the data filtering part.
	Multiple modifications made to all the selected data.
	Creates new data.
	Duplicate the selected data (ask a new name)
	Deletes the selected data (one or many).
	Enables data filtering or not.
	Defines the filter to be applied to the data.

Filtering allows you to display only what is necessary in a table. Several filtering criteria can be combined, as shown below:



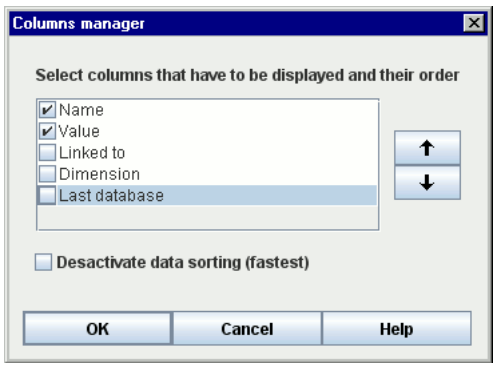
Select **AND** or **OR** to choose the type of association between each line (filter criterion). A line is a Boolean expression divided into 3 parts:

1. the first is the column on which the filter is used;
2. the second is the comparator;
3. the third is the value to which the data will be compared.

If the Boolean expression is true, the data will be kept (displayed); otherwise the data will be masked. When the filter is enabled its value is displayed between < and >.

The data in a column can be sorted by double clicking the header of this column. The first double click will sort the data in ascending order (small triangle pointing upwards). The second double click on the same header will sort the column in descending order (small triangle pointing downwards).

A table can contain many columns, some columns may be unnecessary in certain cases. The "linked to database" column is unnecessary when no database is available. It is thus possible to choose the columns to be displayed and their order. To do this, click right on a table header, or click the **Columns Manager** button, the following window opens:

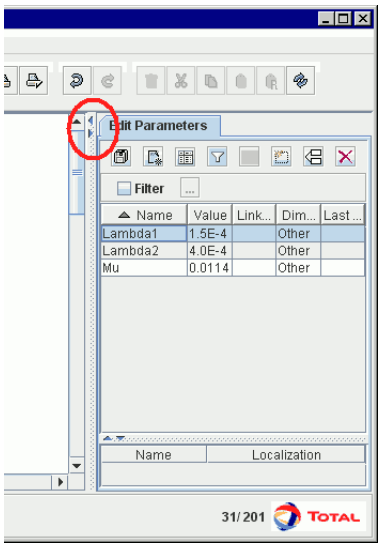


You can choose the columns to be displayed by selecting (or deselecting) the corresponding check boxes. The arrows on the right are used to move the columns up or down in the list to choose the order of the columns. The **Disable data sorting** check box disables the data sorting. This improves the application's performance with very complex models.

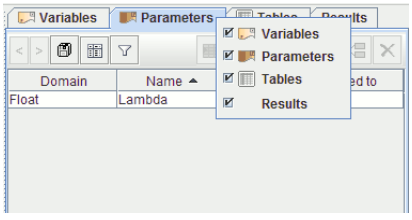
10.2.2. Table accessibility

As mentioned above, the tables can be accessed via the **Data and Computations** menu; in this case, each table is displayed in a separate window.

To avoid having too many windows open, all the tables are grouped together in tabs on the right-hand side of the application. This area can be hidden/displayed using the small arrows above the input zone.



It is possible to choose the tables in this zone by right clicking on the tabs. A contextual menu appears, in which the user can select the tables s/he wishes to display.



10.3. Options of GRIF - SIL

Tools - Application Options menu opens a window containing the following tabs:

10.3.1. Executables

Executables tab enables to specify path to external executables :

- **Editor path** : Specifies text editor path.
- **Mail client** : Enable you to set the mail client to use
- **Automatically open PDF files** : Specifies if PDF reports must be opened with generation.
- **Style-sheet from XML to DocBook.** : Style-sheet allowing converting from XML report to docbook file.
- **Style-sheet from XML to HTML.** : Style-sheet allowing converting from XML report to HTML file.
- **Style-sheet from DocBook to PDF.** : Style-sheet allowing converting from docbook file to PDF file.
- **Moca-RPC path** : Specifies Moca version 12 path.
- **Javaw path** : Path of javaw.exe executable.

10.3.2. Database

Database tab enables to configure database connection :

- **Use DataBase connection for parameters** : Select if database must be use.
- **Name** : Database name will be put into parameter during its update. It enables to know from which database parameter has been lastly updated.
- **JDBC Driver** : Enter name of JDBC driver to be used(sun.jdbc.odbc.JdbcOdbcDriver, oracle.jdbc.driver.OracleDriver, ...).
- **Connection to database** : Database Url.
- **Connection options** : Connection properties.
- **Login** : Login to be used to connect to database.
- **Password** : Password to be used to connect to database.
- **SQL Request** : Request that have to be executed to retrieve data from database.
- **Name of "ID" field** : Name of field containing data ID.
- **Type of ID** : Type of ID field (INTEGER, FLOAT, VARCHAR(32), ...)
- **Name of "name" field** : Name of field containing data name.
- **Name of "value" field** : Name of field containing data value.
- **Name of "description" field** : Name of field containing data description.
- **Name of "dimension" field** : Name of field containing data dimension.
- **Test Connection** : Name of field containing data description.

10.3.3. Language

Language tab enables to choice language :

- **Language** : Language changes are taken into account when option windows is closed.Available language are French and English.

10.3.4. Options

Options tab enables to tune application behavior :

- **Save the options of the current document as default options in the application** : Save options of current doc as application default options.
- **The application manages the default options of the documents. Apply the default options to the current document** : Apply -Application options- to current document.
- **Delay of automatic document saving (in minutes)** : Delay of automatic document saving (in minutes). A null value disables automatic saving.
- **Number of undo** : Specifies number of possible undo/redo.
- **Number of recent files** : Specifies number of files in recent files list.
- **Window display** : Enables separate tables (external) or linked tables (internal).
- **Columns to be resized in tables** : Enables to specify the columns on which space will be taken for resizing.
- **Manage new names to avoid name conflict** : Tries to avoid name conflict, creating new objects whose name is unik (when pasting for example).

- **Add "Copy" suffix for copy-paste** : If Enabled, a "copy" suffix will be added to the name of pasted objects.
- **Synchronize view with tables** : Select objects in tables (on the right) when they are selected in view.
- **Synchronize view with explorer** : Select objects in explorer (on the left) when they are selected in view.
- **Spurious-trip in reports** : Display the spurious trip rate in XLSX and PDF report.

10.3.5. Graphics

Graphics tab enables to modify GUI look :

- **Use Windows look and feel** : Use the look and feel of your operating system instead of java look and feel (GRIF restart is needed).
- **Element Zoom** : Changes graphics size.
- **Comment size** : Changes comment font size.
- **Group size** : Changes group font size
- **Activate smoothing for texts** : Activate anti-aliasing (smoothing) for texts, it can slow the display.
- **Activate smoothing for images** : Activate anti-aliasing (smoothing) for images, it can slow the display.
- **Activate tooltips** : Activate tooltip-system.

10.3.6. Digital format

Digital format tab enables to customize digits display :

- **Display of parameters** : Specifies the display of parameters (number of digits, ...).

10.3.7. Curves

Charts tab enables to change charts drawing :

- **Set graphics borders** : Add borders to charts.
- **Set generic values borders** : Add borders to generic values under charts.
- **Display grid** : Display grid on curves area.
- **Display legends** : Display legends under curves.
- **Drawing zone transparency** : Activate curves area transparency.
- **Graphic transparency** : Activate charts transparency.
- **Title size** : Specifies charts title font size.
- **Generic values size** : Specifies generic values font size.
- **Point size** : Specifies point size on curves.
- **Coordinates size** : Specifies coordinates font size.
- **Legend size** : Specifies legends font size.